Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Informatiksteuerungsorgan des Bundes ISB

A006 - Smartcard

Klassifizierung:	Nicht klassifiziert
Typ:	IKT-Standard
Ausgabedatum:	2016-04-18
Version:	3.0.2
Status:	Genehmigt
Ersetzt:	3.0.1
Verbindlichkeit:	Weisung
Genehmigt durch:	Informatiksteuerungsorgan Bund, am 2016-01-12
Beilagen:	- Beilage 1: Spezifikation BIT : Beilage zum A006 - Beilage 2: Spezifikation BBL: Physikalische Spezifikation und Transponderchip

Inhaltsverzeichnis

Das Informatiksteuerungsorgan Bund erlässt gestützt auf Artikel 17 Absatz 1 der Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung (BinfV) [BinfV] nachfolgende Weisungen.

1 Anwendungsbereich

Dieses Dokument beschreibt die Vorgaben für die von der Bundesverwaltung eingesetzten Smartcards und die für deren Einsatz nötigen Soft- und Hardwareelemente.

2 Geltungsbereich

Der Geltungsbereich der Weisungen ist identisch mit dem Geltungsbereich der BinfV [BinfV].

3 Verbindlichkeit

Der Verbindlichkeitsgrad der einzelnen Vorgaben wird mittels der im Anhang B zusammengestellten, in Grossbuchstaben geschriebenen Schlüsselwörter gekennzeichnet.

4 Definitionen

Secure Desktop: Bildschirmanzeige, die nach dem gleichzeitige Drücken der Tasten Ctrl+Alt+Del angezeigt wird.

Konfektionierung: Das Einbetten des Kryptochip in die Plastikkarte und die weiteren Bearbeitungsschritte für die Fertigstellung der physikalischen Smartcard (z. B. Bedrucken, Laminieren, Programmieren). Das Ergebnis der Konfektionierung wird als Smartcard bezeichnet.

Secure Key Injection (SKI): Diese Methode erlaubt es, geheime Schlüssel von einer Server-Anwendung über einen unsicheren Client PC sicher auf die Smartcard zu senden [SKI].

5 Beschaffung, Konfektionierung, Bestellung

1. Der Kryptochip MUSS durch das Bundesamt für Rüstung (armasuisse), beschafft werden.
2. Der Fertigungsprozess (Konfektionierung) der Smartcard MUSS durch das Bundesamt für Bauten und Logistik (BBL) oder durch die armasuisse erfolgen oder beauftragt werden.
3. Für den Beschaffungs- und Konfektionierungsvorgang jedes Chips und jeder Karte MUSS die Nachvollziehbarkeit gewährleistet sein.
4. Die Bestellung von Smartcards MUSS über das BBL oder die armasuisse erfolgen.

6 Erforderliche Komponenten und Schnittstellen

6.1 Kryptochip

1. Der Kryptochip MUSS als asymmetrisches Verfahren mindestens RSA und als symmetrisches Verfahren mindestens AES unterstützen.
2. Die Schüssellänge für RSA MUSS mindestens 2048 Bit betragen.
3. Die Random Number Generator (RNG) Methode MUSS unter Non-Disclosure Agreement (NDA) einsehbar sein.
4. Das Verfahren der Schlüsselgenerierung auf dem Kryptochip MUSS unter NDA einsehbar sein.
5. Der Schlüssel MUSS mit CKA Attributen markierbar sein (CKA Attribute CKA_SIGN, CKA_ENCRYPT und weitere PKCS#11 Attribute und Objekte).
6. PKCS#11 [PKCS#11] MUSS für CNG/CSP und umgekehrt transparent sein.
7. Ein PIN Unlock MUSS über den Secure Desktop erfolgen können.
8. Der PIN Wechsel MUSS über den Secure Desktop erfolgen können.
9. Der Kryptochip MUSS über die Kette bestehend aus CNG/CSP, Minidriver [SCM] und PC/SC [PC/SC v2.01] ansprechbar sein.
10. Der Kryptochip MUSS über die Kette bestehend aus PKCS#11 [PKCS#11] und PC/SC [PC/SC v2.01] ansprechbar sein.
11. Der Kryptochip MUSS mindestens 64kB Speicher aufweisen.
12. Die Filesystem Partitionierung MUSS bei Initialisierung konfigurierbar und in Private / Public Memory aufteilbar sein oder MUSS dynamisch erfolgen.
13. Der Kryptochip SOLL mindestens über eine EAL 4+ Zertifizierung gemäss den Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur [TAV] verfügen.
14. Es MUSS sowohl eine PIN als auch ein PUK gesetzt werden können.
15. Bei der Initialisierung MUSS sowohl für die PIN als auch für den PUK eine Policy definierbar sein.
16. Der Kryptochip MUSS die Smart Card Minidriver Specification v7 und die Smart Card Minidriver Specification v7.07 [SCM] unterstützen.
17. Der Kryptochip MUSS Secure Key Injection (SKI) [SKI] unterstützen.
18. Der Kryptochip MUSS mindestens von folgenden Betriebssystemen unterstützt werden: Windows 7 32/64 bit, Windows 10 32/64 bit, Windows Server ab 2008.
19. Der Kryptochip SOLL von Linux ab Kernel 2.6 und höher unterstützt werden.

6.2 Smartcard-Reader

1. Der Smartcard-Reader MUSS mindestens an einem USB-Port an den PC angeschlossen werden können.
2. Der Smartcard-Reader MUSS den PC/SC Standard [PC/SC v2.01] erfüllen.
3. Bei der Beschaffung der Büroautomationsgeräte MUSS die beschaffende Stelle die zu beschaffenden Geräte (z. B. Laptops, Tastaturen mit integrierten Smartcard-Readern) auf Kompatibilität mit den in der Bundesverwaltung eingesetzten Smartcards überprüfen. Das Testvorgehen MUSS durch die Swiss Government PKI genehmigt werden. Das Testergebnis MUSS der Swiss Government PKI gemeldet werden.

6.3 Smartcard (physikalische Sicht)

1. Die Smartcard MUSS die Grösse 85,60 mm × 53,98 mm und eine Stärke von 0.76 mm

(gemäss ISO 7810 ID-1) aufweisen.
2. Das BBL MUSS in Abstimmung mit dem BIT und dem ISB die Beilage 2 zu diesem Standard mit den Vorgaben für die Smartcard (physikalische Sicht) erstellen.
3. Das BBL KANN in der Beilage 2 zu diesem Standard auch die optionalen Komponenten und Schnittstellen (z.B. Transponderchip, RFID, Antennen für NFC) beschreiben.

6.4 Zugriff auf Smartcard

1. Unter Windows SOLL als Treiber der Minidriver nach der Smart Card Minidriver Specification v7 oder v7.07 [SCM] eingesetzt werden.
2. Unter Linux DARF der Kryptochip mit PKCS#11 [PKCS#11] angesprochen werden.

7 Allgemeine Bestimmungen

1. Das BIT MUSS die Beilage 1 erarbeiten, aktuell halten und im Intranet des ISB publizieren.
2. Das BBL MUSS die Beilage 2 erarbeiten, aktuell halten und im Intranet des ISB publizieren.
3. Der Antrag für die Aufnahme von nicht zugelassenen Smartcards in die Liste der zugelassenen Smartcards MUSS an den Führungsausschuss Standarddienste Bund (FSD) gemäss dessen Geschäftsreglements gerichtet werden.

8 Schlussbestimmungen

8.1 Aufhebung bisheriger Vorgaben

Der Standard A006 Version 2.13 wird aufgehoben.

8.2 Übergangsbestimmungen

Der Kryptochip DARF unter Windows bis 31.Dezember 2018 mit PKCS#11 [PKCS#11] angesprochen werden.

8.3 Inkrafttreten

Der Standard tritt am Datum der Genehmigung in Kraft.

Anhänge

A. Änderungen gegenüber Vorversion

Vollständige Überarbeitung.

Migration des Standards in die neue Vorlage gemäss P035.

Ergänzung der Beilagen und Anpassung der Beilagenbezeichnungen.

B. Bedeutung der Schlüsselwörter zur Bestimmung des Verbindlichkeitsgrades

Der Verbindlichkeitsgrad der einzelnen Vorgaben wird im Dokument mittels folgender in Grossbuchstaben geschriebenen Schlüsselwörter gekennzeichnet:

MUSS	Vorgabe, die einzuhalten ist (gewährte Ausnahmen ausgenommen)
DARF NICHT	Option, die nicht gewählt werden darf
DARF	Die Option ist explizit erlaubt. Die Nutzer entscheiden, ob sie die Option nutzen möchten. – Betrifft die Vorgabe eine IKT-Lösung, muss der Anbieter der Lösung die Option anbieten.
SOLL	Option, die im Normalfall zu wählen ist. Es kann jedoch ohne Ausnahmegewährung des ISB davon abgewichen werden, insbesondere wenn die Wirtschaftlichkeit oder Sicherheit andernfalls nicht mehr gewährleistet werden können. Die Abweichung von der Vorgabe ist jedoch schriftlich zu begründen.
KANN	Akzeptierte Option. – Betrifft die Vorgabe eine Lösung, entscheidet der Anbieter der Lösung darüber, ob er die Option unterstützen will.

C. Abkürzungen

Kürzel	***Bedeutung***
armasuisse	Bundesamt für Rüstung im Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport
BBL	Bundesamt für Bauten und Logistik im Eidgenössischen Finanzdepartement
BinfV	Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung vom 9. Dezember 2011
BIT	Bundesamt für Informatik und Telekommunikation

Kürzel	***Bedeutung***
CNG	Cryptography Next Generation: wurde mit der Windows Version 7 eingeführt und erlaubt den Einsatz der durch das NIST in der Suite B definierten Algorithmen.
CNG/CSP	Der Crypto Next Generation Key Storage Provider (KSP) und der Microsoft Smart Card Base Cryptographic Service Provider können mit Hilfe des vom Kartenhersteller gelieferten Minidrivers [SCM] auf die Smartcard zugreifen.
DH	Diffie Hellmann, Schlüsselaustauschprotokoll
FSD	Führungsausschuss Standarddienste Bund
ISB	Informatiksteuerungsorgan Bund
ISO	International Standards Organisation
NDA	Non-Disclosure Agreement
NFC	Near Field Communication
PC/SC	Personal Computer – Smartcard Interface
PIN	Persönliche Identifikationsnummer
PKCS#11	Public Key Cryptographic Standard Number 11, von RSA LABORATORIES geschaffener Standard, siehe [PKCS#11]. Die aktuelle Version ist 2.20.
PUK	Personal Unblocking Key
RNG	Random Number Generator
RSA	Kryptosystem, das nach seinen Erfindern Rivest, Shamir und Adleman benannt ist.
SG-PKI	Die Public-Key-Infrastruktur der Bundesverwaltung (Swiss Government PKI) erbringt für die Nutzung des Internets die behördenübergreifende Sicherheit.
SKI	Secure Key Injection
SR	Systematische Sammlung des Bundesrechts

Kürzel	*Bedeutung*
TAV	Technische und administrative Vorschriften über Zertifizierungs-dienste im Bereich der elektronischen Signatur, Anhang zu SR SR 943.032.1

D. Referenzen

[BinfV] Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung vom 09. Dezember 2011 (Stand am 01. Januar 2012); SR 172.010.58
Suche über die SR Nummer unter https://www.admin.ch/gov/de/start/bundesrecht/systematische-sammlung.html

[PC/SC v2.01] PC/SC Workgroup Specifications Overview

http://www.pcscworkgroup.com/specifications/overview.php

[PKCS#11] Cryptographic Token Interface Standard

ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/pkcs-11v2-20.doc

[SCM] Smart Card Minidriver Versions

https://msdn.microsoft.com/en-us/library/windows/hardware/dn631754

[SKI] Secure Key Injection

https://msdn.microsoft.com/en-us/library/windows/hardware/dn468772(v=vs.85).aspx

[TAV] Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur

http://www.bakom.admin.ch/themen/internet/00467/index.html?lang=de